REMARKS

The Examiner has rejected Claims 1-2, 5-6, 8-12, 14-15, 17-19, 21-22, 24 and 26-28 under 35 U.S.C. 102(b) as being anticipated by Hitachi, Ltd. (EP 0893 769 A1). The Examiner has also rejected Claims 3, 4, 13, 20 and 23 under 35 U.S.C. 103(a) as being unpatentable over Hitachi in view of Arnold et al. (U.S. Patent No. 5,440,723). Applicant respectfully disagrees with such rejections.

With respect to independent Claims 1, 9-11 and 23, the Examiner has relied on Col. 5, lines 21-39; Col., 8, lines 48-57 and steps 801-823 in Figure 8 of Hitachi to make a prior art showing of applicant's claimed technique "wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content."

Applicant respectfully asserts that the excerpts relied on by the Examiner merely teach "mov[ing] the data to a computer exclusively used for execution to thereby quarantine the data from the network" and carrying out "a check to determine whether or not [a] digital signature added to the security software is valid." Clearly, quarantining data and determining if a signature is valid, as taught by Hitachi, fails to meet any sort of "scann[ing] with a malicious code detection file received after the potentially malicious content," as claimed by applicant (emphasis added).

In fact, after review of steps 801-823 in Figure 8, applicant notes that the description of such steps in Col. 13, lines 48-51 *teaches away* from applicant's specific claim language. In particular, such excerpt discloses that "the file server 621 is disconnected from the network if there is not a request from the security agent 651 to the security clerk 653" (emphasis added). Applicant emphasizes that a request for a "connection between the file server 621 and the computer 611 via the network 601" is made by the security agent 651 such that "the security agent 651 [is able to transfer] the suspected file 613 to the file server 621" (see Col. 13, lines 44-48). Thus, Hitachi's disclosure of disconnecting the file server from the network except for when a request is

made to transfer a suspected file would make it *impossible* or *unworkable* to allow a "malicious code detection file [to be] received after the potentially malicious content," in the specific manner claimed by applicant.

With respect to the 102 rejection, the Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Hitachi reference, as noted above. A notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

With respect to the 103 rejection, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Applicant has amended Claim 17 to incorporate the following claim language:

"wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content."

Applicant respectfully asserts that such language has not been met by the Hitachi reference relied on by the Examiner, for the reasons argued above with respect to the remaining independent claims. Thus, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. Just by way of example, with respect to Claim 4, the Examiner has relied on Col. 9, lines 61-68 and Col. 10, lines 53-56 in Arnold to make a prior art showing of applicant's claimed technique "wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value."

However, applicant notes that such excerpts relate to "estimated 'false-positive' probabilities" of signatures. Clearly, a probability of a signature creating false-positives, as in Arnold, does not meet applicant's specific claim language, namely "wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value" (emphasis added).

In addition, with respect to Claim 6, the Examiner has relied on Col. 7, lines 34-45 in Hitachi to make a prior art showing of applicant's claimed technique "wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value." Applicant respectfully asserts that such excerpt merely discloses an open key list organized according to type (see Figure 1). The open key list only includes a set open key, an identification name, and a type. However, nowhere in such excerpt or associated

Figure is there any suggestion of an electronic mail message, let alone "an electronic mail message [that] is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value," as specifically claimed by applicant (emphasis added).

With respect to Claim 27, the Examiner has relied on Col. 7, line 46-Col. 8, line 26 along with items 803-804 of Figure 8 in Hitachi to make a prior art showing of applicant's claimed technique "wherein when multiple recipients are to receive a copy of the potentially malicious content over the network, a single copy of the potentially malicious content is quarantined and each of the recipients is placed in a list such that after the potentially malicious content is determined to be clean based on the testing, the single copy is forwarded to each of the recipients." Applicant respectfully asserts that in such excerpt and Figure relied on by the Examiner, the only list disclosed is a stack activation list which is populated with received security software (see, specifically, Col. 8, lines 10-11). Clearly, a stack populated with security software, as in Hitachi, does not meet applicant's claim language where "each of the recipients [of potentially malicious content] is placed in a list such that after the potentially malicious content is determined to be clean based on the testing, the single copy is forwarded to each of the recipients" (emphasis added).

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 29-31 below, which are added for full consideration:

> "wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with the malicious code detection file received after the potentially malicious content and after the potentially malicious content is quarantined" (see Claim 29);
>
> "wherein the malicious code detection file is created after the potentially malicious content is identified such that a latest malicious code detection file is utilized in the scanning of the potentially malicious content" (see Claim 30); and

"wherein the malicious code detection file is created after the potentially malicious content is received such that a latest malicious code detection file is utilized in the scanning of the potentially malicious content" (see Claim 31).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P040/01.254.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100